Remarks by

Lieutenant General Michael D. Barbero
Director, Joint IED Defeat Organization

Delivered at

RUSI Land Warfare Conference
London, United Kingdom

June 8, 2012

Good morning. Thank you for the kind introduction. General Sir Peter Walls, fellow flag officers and general officers, industry leaders, defense institutions, ladies and gentlemen. I appreciate the opportunity to be here today — joining my colleagues Generals Bruce Brealey and Bill Phillips — both comrades from our days in Bagdad — to discuss the future of our armies and how we will define and deliver capabilities moving forward.

I'm General Michael Barbero, Director of the United States Department of Defense's Joint Improvised Explosive Device Defeat Organization. JIEDDO, as it is commonly known, was established in 2006 to focus on the improvised explosive device problem in Iraq and Afghanistan. My organization is singularly focused on this threat and we exist to rapidly field capabilities to reduce the effectiveness of the IED.

Let me say up front, as I look to 2020, it is clear the IED, and the networks that use these weapons, will remain a threat —to our forces and to our homelands — for decades. This threat is global — and growing. To adequately prepare our armies for the future, I believe we need to look at what we have learned over the last decade and apply those lessons to our planning. We must recognize the significant effect IEDs have had during the last decade of combat operations.

We need to examine not only the characteristics of the IED itself but also the networks that employ this device and assess if what we see today in this IED environment — is a window into the future and what lessons, therefore, should be incorporated into the shaping of the Army of 2020.

As General John Allen, commander of ISAF stated bluntly, this is a "very tough mission against an intelligent, resourceful and resilient enemy with patience and little regard for human life." We have seen the insurgency relying increasingly on IEDs as the weapon of choice. In Afghanistan, these devices are the greatest source of casualties — with more than 1,500 IED events per month.

But the IED threat continues to expand well beyond Afghanistan and is truly a global threat with more than 500 IED attacks occurring outside of Iraq and Afghanistan on a monthly basis. Since last year, there were nearly 8,000 global IED events occurring in 112 countries, executed by more than 40 regional and transnational threat networks.

Today's extremist networks that employ IEDs have proven to be resilient, adaptive, interconnected, and violent. Globalization, the internet, and social media have extended the reach of these organizations — providing platforms for recruiting, technical exchanges, training, planning, funding, and social interaction. Their ability to seamlessly communicate and share explosive device recipes; tactics, techniques and procedures; and migrate back and forth — it's really a huge strategic advantage for these threat networks and something that will continue in the future.

While we adhere to Napoleon's dictum to "march to the sound of the guns," these threat networks "march to the signs of insecurity…and take the IED with them." We see this in Colombia, Pakistan, Syria, India, Somalia, Nigeria, and Bahrain among others. Wherever we see turmoil or insecurity, we see the spread of these networks and the spread of IEDs — now and in the future.

We've also seen IED tactics and techniques used by insurgents increase in sophistication and proliferate globally. Take, for example, the explosively formed projectile that we saw in Iraq has made its way to the Gaza Strip, and recently in Somalia — all tracking back to Iran and Iran-supported organizations. Vehicle-borne IEDs that we've seen in the Middle East, we're now seeing in Mexico. And the use of female suicide bombers — pioneered by the Tamil Tigers in Sri Lanka — spread throughout the Middle East, worked its way to Southeast Europe, and most recently have been employed in Somalia and Nigeria.

And, of significance for this audience, ammonium nitrate-based IEDs employed by the Provisional Irish Republican Army in the early 1980s have now proliferated throughout Afghanistan and globally.

These threat networks are going to use whatever is cheapest and most available. Today's IEDs are relatively simple, low-tech devices, which routinely use command wire, pressure plates, or radio-controlled triggers. As you know, many readily available components such as circuit boards, cell phones, and simple electronic transmitters and receivers have legitimate commercial uses, but are easily and increasingly adapted into IEDs.

If these networks can get their hands on commercial explosives, that's what they are going to use. But I tell you, we face a growing commercial off-the-shelf problem — radio-controlled IEDs, cell phones, circuit boards, commercial fertilizers propane tanks, and pressure cookers are all being used.

In Afghanistan, we've started to see improvised blasting caps made from light bulbs. And, fertilizer-based explosives still remain our greatest threat there. 86 percent of IEDs employed in Afghanistan are homemade explosives, and of those, 83 percent are made with ammonium nitrate derived from calcium ammonium nitrate — a common agricultural fertilizer. This fertilizer and other easily procured, dual-use, ubiquitous, hard to detect components present a strategic advantage to our enemies, and a security challenge to all of us.

In the future, devices will likely adopt more sophisticated technology — limited only by one's imagination. Future bomb makers will incorporate such enhancements as ultra-thin and flexible electronics; advanced communications mechanisms such as blue-tooth, Wi-Fi, and broadband; optical initiators; and highly energetic and molecular materials. In addition to more sophisticated technology, threat networks will develop enhanced IED concealment techniques and may even combine IED use with concurrent cyber attacks.

The likelihood of new and developing technology being applied to IEDs and used against the Army of 2020 is certain — and troubling. The ubiquitous nature of IED materials, their low cost and the potential for catastrophic results guarantees the IED will remain a threat and main casualty-producing weapon for decades to come — confronting the Army of 2020 and beyond.

The IED and the threat networks that employ this weapon are a reality of 21st century warfare and we must plan accordingly. So, as we look to the future and begin planning for the Army of 2020, we must ask ourselves, is the IED going to be here for the next decade?

The answer is <u>absolutely</u>. The IED is too cheap, readily available, and easy to construct. We have a whole generation of experienced, savvy, smart bomb-makers who know how to adapt and will continue to take advantage of all available off-the-shelf technology — making devices more lethal and harder to detect and defeat. So the answer is yes — the IED is going to be here.

The next question that should be asked is — will these threat networks try and attack our forces and our homelands in the future? Again, I believe the answer is yes

So, as we look to the future, what are those counter-IED capabilities that must endure to ensure our forces are prepared for the future threat environment?

For my nation, as we look to the post Afghanistan period, to deal with the IED and threat networks, I believe there are five overarching capabilities that should be institutionalized within the Defense Department.

<u>First</u>, we must maintain the ability to <u>rapidly</u> provide counter-IED materiel and non-materiel solutions in response to changes in the IED threat. We must maintain a higher level of institutional agility and leverage the capabilities of our allies.

To give you an example, as dismounted operations increased in Afghanistan, so did severe pelvic injuries to our troops. Thanks to our UK partners, my organization was able to fund and begin to deliver over 200,000 protective outer and undergarments within only a couple of months.

By tapping into an already developed and proven technology, we were able to rapidly respond to an urgent need.

Ensuring our commanders have freedom of maneuver now and in the future is critical. We are operating in an IED environment and that is not going to change anytime soon. To preserve our ability to respond to changes in the IED threat, we must institutionalize a rapid acquisition capability and share new capabilities and emerging technologies with our partners and across the security community. We must deliver capabilities in months — not years.

The second capability that needs to endure is our ability to fuse operational information and intelligence, from all sources, to produce actionable intelligence — analytical products that meet the needs of both our operational commanders and our domestic security partners. This is accomplished through a robust and powerful network of partners with whom analytical tools, methodologies, and most importantly, information and intelligence can be shared to identify, and then exploit, the vulnerabilities of threat networks.

Today, our warfighters and analysts struggle to sort through the explosion of data and proliferation of isolated, independent data feeds — such as full-motion video, imagery, biometrics, intelligence community reporting, open source reporting, raw sensor feeds. We need better techniques to seamlessly share and fuse this data across the attack the network enterprise. The key enabler for achieving seamless sharing of information begins with applying new techniques to enhance data processing upon intake. The better we can sort, or mine, data, the faster our analysts can manipulate this information to produce actionable intelligence for our leaders and actionable evidence for our interagency partners.

We must improve advanced analytics supporting the rapid identification of threat networks activities and our ability to push relevant analysis quickly to expeditionary forces. The speed at which these threat networks operate mandates our ability to produce faster analytical assessments of emerging operational environments to support rapid exploitation.

With this enduring IED and network threat, we must think differently and expand our community of action to empower all domestic and international partners with the ability to share and fuse information. They must see what we see. We must become adept in transforming intelligence into evidence. We cannot go back to our old approach to intelligence — stovepiped and narrowly focused.

Third, we must maintain our ability to train our forces for these enduring threats. Counter-IED and Attack the Network training must endure and be permanently integrated into our individual Service and joint training institutions and centers.

We can provide the best counter-IED capabilities to the warfigher, but without the timely and relevant training component, the full capacity of equipment and tactics will never be realized.

As you know during the Cold War we trained to conduct operations in a nuclear, biological, and chemical environment. As we move to the Army of 2020, we must train to conduct operations in an IED environment, which includes an agile networked enemy. So, we need to identify and institutionalize the individual, leaders, and collective counter-IED and counter-network tasks our Army of 2020 must master.

The fourth enduring capability we must maintain is our ability to conduct relevant and timely collection, analysis, and technical and forensic exploitation of current and emerging IED technologies. This is done through weapons technical intelligence, often referred to as WTI. This capability provides the U.S., U.K., and our international partners a powerful, tiered, systematic process that leads to four important outcomes: force protection, targeting of networks, support to prosecution, and material sourcing.

JIEDDO and our UK partners have built this capability together for the past 8 years. WTI builds knowledge of the networks through DNA, finger prints, trace/fiber, and device technical signatures. There are countless examples of successful WTI-based targeting. Our commanders increasingly focus operations to collect biometric data, and several have referred to it as a "game-

changer." Biometric collections removes the insurgents greatest defense — anonymity — and makes them vulnerable to attribution.

We need to build upon capabilities such as the Counter-IED Theater Exploitation Laboratory in Afghanistan — a European Defense Agency Initiative — and build on the performance of our U.S. and U.K. labs in Afghanistan and at home. Yet, in the US, our intelligence community has not fully embraced nor resourced this as an enduring capability, and unless this changes, our WTI capabilities will wither. As we look toward 2020 and this enduring threat — does this really make sense?

Fifth, and finally, as I mentioned earlier, the enduring global IED threat requires a whole-of-governments approach. As we move forward, we must continue to synchronize counter-threat network capabilities and actions among national, international, and other security stakeholders.

Recognizing the significant threat homemade explosives poses to Coalition and Afghan Security Forces in Afghanistan, we have established an HME Task Force to synchronize intelligence and non-kinetic targeting across the multinational, U.S. interagency spectrum. To allow us to use all tools — freezing assets, blocking access to technology, opening criminal cases, restricting imports and exports — in order to non-kinetically attack the threat networks that employ homemade explosives.

Central to the survival of these threat networks that employ IEDs is money. We are enlisting the help of our U.S. government and international partners, and also engaging private sector business and financial industry executives to identify, disrupt, and dismantle supporting financial networks. Now, and in the future, mapping the financial networks of our adversaries is what allows us to take action. Follow the money, the money trails don't lie. This makes financial intelligence a uniquely effective source to attack on threat networks, and a skill we must grow in the future.

I tell my federal partners there's an IED coming to a major city near you. This statement applies to all of us. There are too many networks, and too many of this generation of bomb-makers who are determined. So, as we consider the Army of 2020, we have to continue to pursue a whole-of-governments approach, knitting together all of the tools we have at our disposal as we work collectively and seamlessly to understand these threat networks and mitigate the effects of the IED.

These five enduring capabilities —

- **Rapid acquisition and fielding;**
- **Operations-intelligence-information fusion**
- **Counter-IED training;**
- **Weapons technical intelligence;**
- **And, a whole-of-governments approach**

— are synergistic and provide a comprehensive response to a complex, asymmetric, and dynamic threat. After all — it takes a network to defeat a network.

Before closing, there are a couple questions about the future I believe we should collectively explore.

First — and the most critical — how do we institutionalize counter-IED capabilities as we build the Army of 2020?

My greatest concern, in this time of diminishing resources, is that nations — including my own — will allow hard-won counter-IED capabilities to attrite. <u>We must not let this happen.</u> We need to stay ahead of the enemy by preparing for future threats. It comes down to risk versus cost. How much risk are we willing to accept? And at what future cost?

Admiral Stavridis characterized the current level of counter-IED competency as having produced, I quote, a "notch generation." This experienced, combat-tested, technologically advanced pool of veterans possesses a unique, unprecedented level of talent forged during the last 10 years of operational experience. We must not lose this competency.

So, how do we apply the lessons we have learned and institutionalize the best counter-IED practices to ensure our armies of 2020 are prepared for the asymmetric threats of the future?

The second question, how do we change our approach to training — individual, collective, and leader training? How do we integrate counter-IED training into our institutions? Today, frankly, we are not doing so well, effective counter-IED training remains our biggest counter-IED gap.

As I said earlier, our forces will operate in an IED environment in the future. As one Brigade Commander in Afghanistan told me, "the IED is not just a weapon on the battlefield — it is the battlefield." During Cold War we trained and equipped our forces to operate in a nuclear, biological, chemical environment. For our armies of 2020, we need to train to operate in the IED environment.

As the great British Soldier J.F.C. Fuller said, I quote, "no new weapon can be introduced without changing conditions, and every change in conditions will demand a modification in the application of the principles of war" end of quote. The IED and the networks that employ them are a fixture on the battlefield — it is our responsibility to adapt institutions and train our forces accordingly. So, how do we do this in building the Army of 2020?

In closing, if you leave here today with only one take-away — it is that the IED threat is global and it is enduring. Addressing this threat requires innovative and creative solutions by all of us.

And, while no one can predict for certain what the future threat environment will look like — I can confidently say that the IED will be a factor in any future operation.

In the 20th century, artillery was the main casualty producer on the battlefield. I believe "The IED is the artillery of the 21st century."

I appreciate your time and attention this morning. I am happy to entertain any question you may have.

Thank you.